PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-326166

(43)Date of publication of application : 16.12.1997

(51)Int.Cl. G11B 20/10

G09C 1/00

H04L 9/08

(21)Application number : 08-144460

(22)Date of filing : 06.06.1996

(71)Applicant : MITSUBISHI ELECTRIC CORP

(72)Inventor : SAKAI YASUYUKI

YAMAGISHI ATSUHIRO

TAKEDA EISAKU

(54) METHOD AND SYSTEM FOR PROTECTING COPYRIGHT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a copyright protection method capable of protecting a right of an author.

SOLUTION: In a transmission side of digital information, the digital information is ciphered by a first ciphering key, and the first ciphering key is ciphered by a second ciphering key. Then, the ciphered digital information is added with the ciphered first ciphering key to be transmitted. Then, in the receiving side of the digital information, the ciphered first ciphering key is deciphered by the second

ciphering key, and the ciphered digital information is deciphered by the first ciphering key obtained by the result of the deciphering.

LEGAL STATUS

[Date of request for examination]	16.02.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	abandonment
[Date of final disposal for application]	18.01.2002
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] The step which enciphers said digital information with the 1st encryption key in the transmitting side of digital information, Have the step which enciphers said 1st encryption key with the 2nd encryption key, and the step which adds said 1st enciphered encryption key to said enciphered digital

information, and is transmitted to it, and it sets to the receiving side of said digital information. The protection-of-copyrights approach characterized by having the step which decodes said 1st enciphered encryption key using said 2nd encryption key, and the step which decodes said enciphered digital information using the 1st encryption key obtained as a result of this decode.

[Claim 2] The protection-of-copyrights approach according to claim 1 characterized by using the encryption key out of which the transmitting side of said digital information and the receiving side came, respectively, and which was beforehand held as said 2nd encryption key.

[Claim 3] The protection-of-copyrights approach according to claim 1 characterized by using the encryption key given as said 2nd encryption key by equipment different from the transmitting side of said digital information, and a receiving side.

[Claim 4] The copyright protection system equipped with the following elements.

(a) The sending set equipped with the following means.

(a1) A means to encipher digital information with the 1st encryption key;

(a2) A means to encipher said 1st encryption key with the 2nd encryption key;

(a3) A means to add said 1st enciphered encryption key to said enciphered digital information, and to transmit to it.

(b) The receiving set equipped with the following means.

(b1) A means to decode said 1st enciphered encryption key using said 2nd encryption key;

(b2) A means to decode said enciphered digital information using the 1st encryption key obtained as a result of decode.

[Claim 5] The copyright protection system according to claim 4 characterized by using the encryption key out of which the transmitting side of said digital information and the receiving side came, respectively, and which was beforehand held as said 2nd encryption key.

[Claim 6] The copyright protection system according to claim 4 characterized by using the encryption key given as said 2nd encryption key by equipment different

from the transmitting side of said digital information, and a receiving side.

[Claim 7] The copyright protection system equipped with the following elements.

(a) The 1st equipment equipped with the following elements.

(a1) Key information on this 1st equipment proper;

(a2) An encryption key generation means to generate a key;

(a3) An encryption means to use initial value as an encryption key, and to encipher said generated key and to encipher said key information by using this enciphered key as an encryption key;

(a4) A transmitting means to transmit said enciphered key and said enciphered key information to the 2nd equipment and 3rd equipment.

(b) The 2nd equipment equipped with the following elements.

(b1) A pseudo-random-number generation means to generate the pseudo-random number;

(b2) A decode means to decode said transmitted key using initial value, and to decode said enciphered key information using this decoded key;

(b3) An encryption means to use said generated pseudo-random number as an encryption key, and to encipher digital information and to encipher said generated pseudo-random number by using said decoded key information as an encryption key;

(b4) A transmitting means to transmit said enciphered digital information and said enciphered pseudo-random number to the 3rd equipment.

(c) The 3rd equipment equipped with the following elements.

(c1) A decode means to decode the key information transmitted by the transmitting means of said 1st equipment, to decode the pseudo-random number transmitted by the transmitting means of said 2nd equipment using this decoded key information, and to decode the digital information transmitted by the transmitting means of said 2nd equipment using this decoded pseudo-random number.

[Claim 8] The encryption key generation means of said 1st equipment is a copyright protection system according to claim 7 characterized by generating the

encryption key of a proper to a system.

[Claim 9] It is the copyright protection system according to claim 7 characterized by for the encryption key generation means of said 1st equipment to generate an encryption key using ID information which identifies said 2nd and 3rd equipment, and for the decode means of said 2nd equipment to decode said enciphered key information using the encryption key generated by said encryption key generation means.

[Claim 10] It is the copyright protection system according to claim 7 characterized by for the encryption key generation means of said 1st equipment to generate an encryption key using ID information which identifies said 1st, 2nd, and 3rd equipment, and for the decode means of said 2nd equipment to decode said enciphered key information using the encryption key generated by said encryption key generation means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention prevents the unjust duplicate of data and relates to the protection-of-copyrights approach and copyright protection system which can protect an author's access.

[0002]

[Description of the Prior Art] The equipment which reproduces the conventional DVD (Digital Video Disc) is explained.

[0003] Drawing 3 is the conventional optical disc system for reproducing DVD. drawing -- setting -- 301 -- for a CD-ROM decoder and 304, as for an error correction circuit and 306, a demodulator circuit and 305 are [a DVD regenerative apparatus and 302 / a disk and 303 / a multiplexer and 307] bus

interfaces. The DVD regenerative apparatus 301 is constituted so that DVD and the disk of both CD-ROMs can be played. Next, actuation is explained. The data by which reading appearance was carried out from the disk 302 are inputted into the CD-ROM decoder 303 and a demodulator circuit 304. In the CD-ROM decoder 303, the recovery in the case of CD-ROM and an error correction are performed. In a demodulator circuit 304, the signal by which reading appearance was carried out is recovered from a disk 302 to digital data. The data to which it restored are inputted into the error correction circuit 305, and perform the error correction of the data of a DVD format. In a multiplexer 306, data are chosen according to any of DVD and CD-ROM disks 302 are, and it outputs to the bus interface 307.

[0004]

[Problem(s) to be Solved by the Invention] The optical disc system which reproduces the conventional DVD did not process at all the digital data currently recorded on the disk, but it was reproducing it as it was recorded by it. Therefore, there was a trouble that it was easy to make the duplicate of the data currently recorded on the disk, and it was difficult to protect the access of the author of data.

[0005] The object of this invention is difficult to have been made in order to solve the starting trouble, and to make the duplicate of data, and it is to obtain the protection-of-copyrights approach and copyright protection system which can protect an author's access.

[0006]

[Means for Solving the Problem] The protection-of-copyrights approach concerning claim 1 of this invention is set to the transmitting side of digital information. The step which enciphers said digital information with the 1st encryption key, and the step which enciphers said 1st encryption key with the 2nd encryption key, Have the step which adds said 1st enciphered encryption key to said enciphered digital information, and is transmitted to it, and it sets to the receiving side of said digital information. It has the step which decodes said

1st enciphered encryption key using said 2nd encryption key, and the step which decodes said enciphered digital information using the 1st encryption key obtained as a result of this decode.

[0007] The encryption key out of which the transmitting side of said digital information and the receiving side came, respectively and which was beforehand held as said 2nd encryption key is used for the protection-of-copyrights approach concerning claim 2 of this invention.

[0008] The encryption key given as said 2nd encryption key by equipment with another transmitting side and receiving side of said digital information is used for the protection-of-copyrights approach concerning claim 3 of this invention.

[0009] The copyright protection system concerning claim 4 of this invention is equipped with the following elements.

(a) The sending set equipped with the following means.

(a1) A means to encipher digital information with the 1st encryption key;

(a2) A means to encipher said 1st encryption key with the 2nd encryption key;

(a3) A means to add said 1st enciphered encryption key to said enciphered digital information, and to transmit to it.

(b) The receiving set equipped with the following means.

(b1) A means to decode said 1st enciphered encryption key using said 2nd encryption key;

(b2) A means to decode said enciphered digital information using the 1st encryption key obtained as a result of decode.

[0010] The encryption key out of which the transmitting side of said digital information and the receiving side came, respectively and which was beforehand held as said 2nd encryption key is used for the copyright protection system concerning claim 5 of this invention.

[0011] The encryption key given as said 2nd encryption key by equipment with another transmitting side and receiving side of said digital information is used for the copyright protection system concerning claim 6 of this invention.

[0012] The copyright protection system concerning claim 7 of this invention is

equipped with the following elements.

(a) The 1st equipment equipped with the following elements.

(a1) Key information on this 1st equipment proper;

(a2) An encryption key generation means to generate a key;

(a3) An encryption means to use initial value as an encryption key, and to encipher said generated key and to encipher said key information by using this enciphered key as an encryption key;

(a4) A transmitting means to transmit said enciphered key and said enciphered key information to the 2nd equipment and 3rd equipment.

(b) The 2nd equipment equipped with the following elements.

(b1) A pseudo-random-number generation means to generate the pseudo-random number;

(b2) A decode means to decode said transmitted key using initial value, and to decode said enciphered key information using this decoded key;

(b3) An encryption means to use said generated pseudo-random number as an encryption key, and to encipher digital information and to encipher said generated pseudo-random number by using said decoded key information as an encryption key;

(b4) A transmitting means to transmit said enciphered digital information and said enciphered pseudo-random number to the 3rd equipment.

(c) The 3rd equipment equipped with the following elements.

(c1) A decode means to decode the key information transmitted by the transmitting means of said 1st equipment, to decode the pseudo-random number transmitted by the transmitting means of said 2nd equipment using this decoded key information, and to decode the digital information transmitted by the transmitting means of said 2nd equipment using this decoded pseudo-random number.

[0013] The copyright protection system concerning claim 8 of this invention equips a system with an encryption key generation means to generate the encryption key of a proper.

[0014] The copyright protection system concerning claim 9 of this invention is equipped with an encryption key generation means generate an encryption key using ID information which identifies said 2nd and 3rd equipment, and is equipped with a decode means decode said enciphered key information using the encryption key generated by said encryption key generation means, in said 2nd equipment in said 1st equipment.

[0015] The copyright protection system concerning claim 10 of this invention is equipped with an encryption key generation means generate an encryption key using ID information which identifies said 1st, 2nd, and 3rd equipment, and is equipped with a decode means decode said enciphered key information using the encryption key generated by said encryption key generation means, in said 2nd equipment in the 1st equipment.

[0016]

[Embodiment of the Invention]

The gestalt of 1 operation of the protection-of-copyrights approach by gestalt 1. this invention of operation is explained based on drawing 1 . Drawing 1 is the flow chart of the protection-of-copyrights approach by the gestalt of this operation.

[0017] Next, actuation is explained. First, the 2nd common encryption key is shared and held by the transmitting side and receiving side of digital information. The transmitting side of digital information prepares the 1st encryption key first. Next, digital information is enciphered using this 1st encryption key. Next, the 1st encryption key is enciphered with the 2nd encryption key currently shared and held. Next, the 1st enciphered encryption key is added to the enciphered digital information, and it transmits to it. The receiving side of digital information performs the next actuation. First, the 1st encryption key enciphered with the 2nd encryption key currently shared is decoded. Next, digital information is decoded using the 1st decoded encryption key.

[0018] By enciphering digital information as mentioned above and transmitting, an informational unjust duplicate can be prevented and an informational author's access can be protected.

[0019] With the gestalt 1 of the gestalt 2. aforementioned implementation of operation, although the 2nd encryption key was beforehand shared by the transmitting side and the receiving side, the 3rd person other than a transmitting side and a receiving side can also supply it.

[0020] The gestalt of 1 operation of the copyright protection system by gestalt 3. this invention of operation is explained based on drawing 2 . Drawing 2 is the block diagram of the copyright protection system by the gestalt of this operation. In drawing, 201 is the 1st equipment, for example, is pocket mold information record media, such as an IC card and a PC card. 202 is peculiar every equipment [the] 201, and, as for the key information on secrecy, 1st ID information that 203 identifies the 1st equipment 201, an encryption key generation means by which 204 generates an encryption key, 1st encryption means by which 205 enciphers the key information 202, and 206, the 1st decode means and 207 are the 1st interface. 208 is the 2nd equipment, for example, is DVD. For a pseudo-random-number generation means and 211, as for the 2nd decode means and 213, the 2nd encryption means and 212 are [209 / 2nd ID information and 210 / the 2nd interface and 214] digital information. The 2nd equipment 208 enciphers digital information 214, and is transmitted. 215 is the 3rd equipment which receives and decodes the digital information 214 which enciphered with the 2nd equipment 208 and was transmitted, for example, is a personal computer which a user uses. As for 216, 3rd ID information and 217 are initial value with which the 3rd decode means and 218 are stored in the 3rd interface, and 219 is stored in the 1st - the 3rd equipment, respectively.

[0021] Next, actuation is explained. First, the procedure in which three equipments, the 1st equipment 201, the 2nd equipment 208, and the 3rd equipment 215, share the key information 202 is explained. The key information 202 on a proper, the 1st ID information 203, and initial value 219 are beforehand written in the 1st equipment 201. The 2nd ID information 209 and initial value 219 are beforehand written in the 2nd equipment 208. The 3rd ID information 216 and initial value 219 are beforehand written in the 3rd equipment 215. Initial value

219 is a common value in the 1st equipment 201, 2nd equipment 208, and 3rd equipment 215. First, an encryption key is generated in the encryption key generation means 204 of the 1st equipment 201, initial value 219 is enciphered as an encryption key with the 1st encryption means 205, and the encryption key is transmitted to the 2nd equipment 208 and 3rd equipment 215 through the 1st interface 207. It is decoded with the 2nd equipment 208 and 3rd equipment 215, and the encryption key generated in the encryption key generation means 204 is a key of a proper, and is shared between three equipments by three equipments which constitute a system. Next, using this shared encryption key, the key information 202 is enciphered in the 1st encryption means 205, and it is transmitted to the 2nd equipment 208 and 3rd equipment 215 through the 1st interface 207. Next, in the 2nd decode means 212 and the 3rd decode means 217, the enciphered key information 202 is decoded and the key information 202 is shared by three equipments.

[0022] Next, the procedure of transmitting the digital information 214 of the 2nd equipment 208 to the 3rd equipment 215 is explained. First, the pseudo-random number is generated in the pseudo-random-number generation means 210, and digital information 214 is enciphered by using the generated pseudo-random number as an encryption key. The generated pseudo-random number is enciphered with the 2nd encryption means 211 by using key information 202 as an encryption key. The digital information 214 enciphered as the enciphered pseudo-random number is transmitted to the 3rd equipment 215 through the 2nd interface 213. With the 3rd equipment 215, the pseudo-random number enciphered first is decoded using the key information 202 currently shared. Next, the enciphered digital information 214 is decoded using the decoded pseudo-random number, and the original digital information 214 is acquired. Since it is enciphered when transmitting digital information, the copyright protection system of the gestalt of this operation can prevent the unjust duplicate of digital information, and can protect an author's access.

[0023] In the 2nd equipment 208 and 3rd equipment 215, although the shared

key information 202 was held, if it is made to hold only when transmitting digital information 214, and transmission is completed, when eliminating from the inside of equipment and starting the next transmission, it can share between the gestalt 3 of the gestalt 4. aforementioned implementation of operation again.

[0024] Although initial value 219 was used as the encryption key with the gestalt 3 of the gestalt 5. aforementioned implementation of operation when transmitting the key information 202 to the 2nd equipment 208 and 3rd equipment 215 First, transmit the 3rd ID information 216 which the 2nd ID information 209 which the 2nd equipment 208 holds, and the 3rd equipment 215 hold to the first equipment [1st] 201, and it sets to the 1st equipment 201. The key information 202 which only the 1st equipment 201 holds based on the 2nd ID information 209 and the 3rd ID information 216 which have been sent from the 1st ID information 203, 2nd equipment 208, and 3rd equipment 215 as a parameter of secrecy A new encryption key can be generated in the encryption key generation means 204, and this can also be used instead of initial value 219.

[0025] What is necessary is just to perform as follows the encryption key generated with the encryption key generation means 205 in order to encipher the key information 202 with the gestalt 3 of the gestalt 6. aforementioned implementation of operation, when either of these three equipments interchanges to another equipment although held with the 1st equipment 201, 2nd equipment 208, and 3rd equipment 215. First, the encryption key generation means 204 generates a new encryption key using the 1st ID information 203, the 2nd ID information 209, and the 3rd ID information 216. Next, initial value 219 is enciphered as an encryption key with the 1st encryption means 205, and the generated encryption key is transmitted to the 2nd equipment 208 and 3rd equipment 215. It decodes using initial value 219 and the new encryption key generated with the encryption key generation means 204 is shared by the 2nd equipment 208 and 3rd equipment 215.

[0026] DVD (Digital Video Disc), CD-ROM, etc. can also use the protection-of-copyrights approach of the gestalten 1-6 the gestalt 7. aforementioned

implementation operation, and a copyright protection system for the regenerative apparatus of a digital information record medium at large. Moreover, although the 1st equipment 201 was used as pocket mold information record media, such as an IC card and a PC card, it should just be the record medium which can hold the key information 202 in secrecy.

[0027]

[Effect of the Invention] As mentioned above, the protection-of-copyrights approach and copyright protection system by this invention can prevent the unjust duplicate of digital information, and are effective in the ability to protect an author's access.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing explaining the protection-of-copyrights approach of this invention.

[Drawing 2] It is the block diagram of the copyright protection system of this invention.

[Drawing 3] It is the block diagram of the conventional optical disc system.

[Description of Notations]

201 1st Equipment, 202 Key Information, 203 1st ID Information, 204 An encryption key generation means, 205 The 1st encryption means, 206 The 1st decode means, The 207 1st interface, 208 The 2nd equipment, 209 2nd ID information, 210 A pseudo-random-number generation means, 211 The 2nd encryption means, 212 The 2nd decode means, 213 The 2nd interface, 214 Digital information, 215 The 3rd equipment, 216 3rd ID information, 217 The 3rd decode means, 218 The 3rd interface, 219 Initial value.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平9－326166

(43)公開日　平成９年(1997)12月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ１１Ｂ　20/10		7736－5D	Ｇ１１Ｂ　20/10	Ｈ	
Ｇ０９Ｃ　1/00	６３０	7259－5J	Ｇ０９Ｃ　1/00	６３０Ｄ	
		7259－5J		６３０Ａ	
Ｈ０４Ｌ　9/08			Ｈ０４Ｌ　9/00	６０１Ｄ	
				６０１Ａ	

審査請求　未請求　請求項の数10　ＯＬ　（全７頁）

(21)出願番号　特願平8－144460

(22)出願日　平成８年(1996)６月６日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　酒井　康行
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　山岸　篤弘
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　竹田　栄作
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

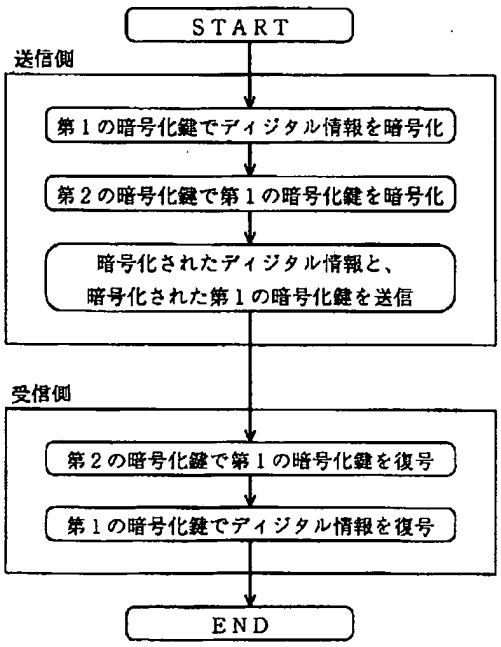
(74)代理人　弁理士　宮田　金雄　（外３名）

(54)【発明の名称】　著作権保護方法及び著作権保護システム

(57)【要約】

【課題】　著作者の権利を保護できる著作権保護方法を得る。

【解決手段】　ディジタル情報の送信側において、前記ディジタル情報を第１の暗号化鍵で暗号化するステップと、第２の暗号化鍵で前記第１の暗号化鍵を暗号化するステップと、前記暗号化されたディジタル情報に前記暗号化された第１の暗号化鍵を付加して送信するステップとを備え、前記ディジタル情報の受信側において、前記第２の暗号化鍵を用いて前記暗号化された第１の暗号化鍵を復号するステップと、この復号の結果得られた第１の暗号化鍵を用いて前記暗号化されたディジタル情報を復号するステップとを備えたものである。



【特許請求の範囲】
【請求項１】　ディジタル情報の送信側において、第１の暗号化鍵で前記ディジタル情報を暗号化するステップと、第２の暗号化鍵で前記第１の暗号化鍵を暗号化するステップと、前記暗号化されたディジタル情報に前記暗号化された第１の暗号化鍵を付加して送信するステップとを備え、
前記ディジタル情報の受信側において、前記第２の暗号化鍵を用いて前記暗号化された第１の暗号化鍵を復号するステップと、この復号の結果得られた第１の暗号化鍵を用いて前記暗号化されたディジタル情報を復号するステップとを備えたことを特徴とする著作権保護方法。
【請求項２】　前記第２の暗号化鍵として、前記ディジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いることを特徴とする請求項１に記載の著作権保護方法。
【請求項３】　前記第２の暗号化鍵として、前記ディジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いることを特徴とする請求項１に記載の著作権保護方法。
【請求項４】　以下の要素を備えた著作権保護システム。
（ａ）以下の手段を備えた送信装置。
（ａ１）第１の暗号化鍵でディジタル情報を暗号化する手段；
（ａ２）第２の暗号化鍵で前記第１の暗号化鍵を暗号化する手段；
（ａ３）前記暗号化されたディジタル情報に前記暗号化された第１の暗号化鍵を付加して送信する手段。
（ｂ）以下の手段を備えた受信装置。
（ｂ１）前記第２の暗号化鍵を用いて前記暗号化された第１の暗号化鍵を復号する手段；
（ｂ２）復号の結果得られた第１の暗号化鍵を用いて前記暗号化されたディジタル情報を復号する手段。
【請求項５】　前記第２の暗号化鍵として、前記ディジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いることを特徴とする請求項４に記載の著作権保護システム。
【請求項６】　前記第２の暗号化鍵として、前記ディジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いることを特徴とする請求項４に記載の著作権保護システム。
【請求項７】　以下の要素を備えた著作権保護システム。
（ａ）以下の要素を備えた第１の装置。
（ａ１）この第１の装置固有の鍵情報；
（ａ２）鍵を生成する暗号化鍵生成手段；
（ａ３）初期値を暗号化鍵として前記生成した鍵を暗号化し、この暗号化した鍵を暗号化鍵として前記鍵情報を暗号化する暗号化手段；
（ａ４）前記暗号化した鍵及び前記暗号化した鍵情報を第２の装置と第３の装置に送信する送信手段。
（ｂ）以下の要素を備えた第２の装置。
（ｂ１）擬似乱数を生成する擬似乱数生成手段；
（ｂ２）初期値を用いて前記送信された鍵を復号し、この復号した鍵を用いて前記暗号化した鍵情報を復号する復号手段；
（ｂ３）前記生成した擬似乱数を暗号化鍵としてディジタル情報を暗号化し、前記復号した鍵情報を暗号化鍵として前記生成した擬似乱数を暗号化する暗号化手段；
（ｂ４）前記暗号化したディジタル情報及び前記暗号化した擬似乱数を第３の装置に送信する送信手段。
（ｃ）以下の要素を備えた第３の装置。
（ｃ１）前記第１の装置の送信手段により送信された鍵情報を復号し、この復号した鍵情報を用いて前記第２の装置の送信手段により送信された擬似乱数を復号し、この復号した擬似乱数を用いて前記第２の装置の送信手段により送信されたディジタル情報を復号する復号手段。
【請求項８】　前記第１の装置の暗号化鍵生成手段は、システムに固有の暗号化鍵を生成することを特徴とする請求項７に記載の著作権保護システム。
【請求項９】　前記第１の装置の暗号化鍵生成手段は、前記第２及び第３の装置を識別するＩＤ情報を用いて暗号化鍵を生成し、
前記第２の装置の復号手段は、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号することを特徴とする請求項７に記載の著作権保護システム。
【請求項１０】　前記第１の装置の暗号化鍵生成手段は、前記第１、第２及び第３の装置を識別するＩＤ情報を用いて暗号化鍵を生成し、
前記第２の装置の復号手段は、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号することを特徴とする請求項７に記載の著作権保護システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データの不正な複製を防ぎ、著作者の権利を保護できる著作権保護方法及び著作権保護システムに関する。
【０００２】
【従来の技術】従来のＤＶＤ（Ｄｉｇｉｔａｌ Ｖｉｄｅｏ Ｄｉｓｃ）を再生する装置について説明する。
【０００３】図３は、ＤＶＤを再生するための従来の光ディスクシステムである。図において３０１はＤＶＤ再生装置、３０２はディスク、３０３はＣＤ－ＲＯＭデコーダ、３０４は復調回路、３０５は誤り訂正回路、３０６はマルチプレクサ、３０７はバスインタフェースである。ＤＶＤ再生装置３０１はＤＶＤとＣＤ－ＲＯＭの両方のディスクを再生できるように構成されている。次に

動作を説明する。ディスク３０２から読み出されたデータは、ＣＤ－ＲＯＭデコーダ３０３および復調回路３０４に入力される。ＣＤ－ＲＯＭデコーダ３０３ではＣＤ－ＲＯＭの場合の復調、誤り訂正が行われる。復調回路３０４ではディスク３０２から読み出された信号をディジタルデータに復調する。復調されたデータは、誤り訂正回路３０５に入力され、ＤＶＤフォーマットのデータの誤り訂正を行う。マルチプレクサ３０６では、ディスク３０２がＤＶＤ、ＣＤ－ＲＯＭのいずれであるかに応じてデータを選択し、バスインタフェース３０７に出力する。

【０００４】

【発明が解決しようとする課題】従来のＤＶＤを再生する光ディスクシステムは、ディスクに記録されているディジタルデータを何ら加工せず、記録されているままに再生していた。そのため、ディスクに記録されているデータの複製を作ることが容易であり、データの著作者の権利を保護することが困難であるという問題点があった。

【０００５】本発明の目的は、係る問題点を解決するためになされたもので、データの複製を作ることが困難で、著作者の権利を保護することができる著作権保護方法及び著作権保護システムを得ることにある。

【０００６】

【課題を解決するための手段】本発明の請求項１に係る著作権保護方法は、ディジタル情報の送信側において、第１の暗号化鍵で前記ディジタル情報を暗号化するステップと、第２の暗号化鍵で前記第１の暗号化鍵を暗号化するステップと、前記暗号化されたディジタル情報に前記暗号化された第１の暗号化鍵を付加して送信するステップとを備え、前記ディジタル情報の受信側において、前記第２の暗号化鍵を用いて前記暗号化された第１の暗号化鍵を復号するステップと、この復号の結果得られた第１の暗号化鍵を用いて前記暗号化されたディジタル情報を復号するステップとを備えたものである。

【０００７】本発明の請求項２に係る著作権保護方法は、前記第２の暗号化鍵として、前記ディジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いるものである。

【０００８】本発明の請求項３に係る著作権保護方法は、前記第２の暗号化鍵として、前記ディジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いるものである。

【０００９】本発明の請求項４に係る著作権保護システムは、以下の要素を備えたものである。

（ａ）以下の手段を備えた送信装置。

（ａ１）第１の暗号化鍵でディジタル情報を暗号化する手段；

（ａ２）第２の暗号化鍵で前記第１の暗号化鍵を暗号化する手段；

（ａ３）前記暗号化されたディジタル情報に前記暗号化された第１の暗号化鍵を付加して送信する手段。

（ｂ）以下の手段を備えた受信装置。

（ｂ１）前記第２の暗号化鍵を用いて前記暗号化された第１の暗号化鍵を復号する手段；

（ｂ２）復号の結果得られた第１の暗号化鍵を用いて前記暗号化されたディジタル情報を復号する手段。

【００１０】本発明の請求項５に係る著作権保護システムは、前記第２の暗号化鍵として、前記ディジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いるものである。

【００１１】本発明の請求項６に係る著作権保護システムは、前記第２の暗号化鍵として、前記ディジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いるものである。

【００１２】本発明の請求項７に係る著作権保護システムは、以下の要素を備えたものである。

（ａ）以下の要素を備えた第１の装置。

（ａ１）この第１の装置固有の鍵情報；

（ａ２）鍵を生成する暗号化鍵生成手段；

（ａ３）初期値を暗号化鍵として前記生成した鍵を暗号化し、この暗号化した鍵を暗号化鍵として前記鍵情報を暗号化する暗号化手段；

（ａ４）前記暗号化した鍵及び前記暗号化した鍵情報を第２の装置と第３の装置に送信する送信手段。

（ｂ）以下の要素を備えた第２の装置。

（ｂ１）擬似乱数を生成する擬似乱数生成手段；

（ｂ２）初期値を用いて前記送信された鍵を復号し、この復号した鍵を用いて前記暗号化した鍵情報を復号する復号手段；

（ｂ３）前記生成した擬似乱数を暗号化鍵としてディジタル情報を暗号化し、前記復号した鍵情報を暗号化鍵として前記生成した擬似乱数を暗号化する暗号化手段；

（ｂ４）前記暗号化したディジタル情報及び前記暗号化した擬似乱数を第３の装置に送信する送信手段。

（ｃ）以下の要素を備えた第３の装置。

（ｃ１）前記第１の装置の送信手段により送信された鍵情報を復号し、この復号した鍵情報を用いて前記第２の装置の送信手段により送信された擬似乱数を復号し、この復号した擬似乱数を用いて前記第２の装置の送信手段により送信されたディジタル情報を復号する復号手段。

【００１３】本発明の請求項８に係る著作権保護システムは、システムに固有の暗号化鍵を生成する暗号化鍵生成手段を備えたものである。

【００１４】本発明の請求項９に係る著作権保護システムは、前記第１の装置において、前記第２及び第３の装置を識別するＩＤ情報を用いて暗号化鍵を生成する暗号化鍵生成手段を備え、前記第２の装置において、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号する復号手段を備えたものであ

る。

【００１５】本発明の請求項１０に係る著作権保護システムは、第１の装置において、前記第１、第２及び第３の装置を識別するＩＤ情報を用いて暗号化鍵を生成する暗号化鍵生成手段を備え、前記第２の装置において、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号する復号手段を備えたものである。

【００１６】

【発明の実施の形態】

実施の形態１．本発明による著作権保護方法の一実施の形態を図１に基づいて説明する。図１は、本実施の形態による著作権保護方法のフローチャートである。

【００１７】次に動作を説明する。まず、ディジタル情報の送信側と受信側とで、共通の第２の暗号化鍵を共有し、保持しておく。ディジタル情報の送信側は、まず第１の暗号化鍵を用意する。次にこの第１の暗号化鍵を用いてディジタル情報を暗号化する。次に、共有し保持されている第２の暗号化鍵で第１の暗号化鍵を暗号化する。次に、暗号化されたディジタル情報に、暗号化された第１の暗号化鍵を付加して送信する。ディジタル情報の受信側は、次の動作を行う。まず、共有されている第２の暗号化鍵で暗号化された第１の暗号化鍵を復号する。次に、復号された第１の暗号化鍵を用いて、ディジタル情報を復号する。

【００１８】以上のようにディジタル情報を暗号化して送信することにより、情報の不正な複製を防ぐことができ、情報の著作者の権利を保護することができる。

【００１９】実施の形態２．前記実施の形態１では、第２の暗号化鍵はあらかじめ送信側と受信側で共有されていたが、送信側、受信側以外の第３者が供給することもできる。

【００２０】実施の形態３．本発明による著作権保護システムの一実施の形態を、図２に基づいて説明する。図２は、本実施の形態による著作権保護システムの構成図である。図において、２０１は第１の装置であり、例えばＩＣカードおよびＰＣカードなどの携帯型情報記録媒体である。２０２は第１の装置２０１毎に固有でかつ秘密の鍵情報、２０３は第１の装置２０１を識別する第１のＩＤ情報、２０４は暗号化鍵を生成する暗号化鍵生成手段、２０５は鍵情報２０２を暗号化する第１の暗号化手段、２０６は第１の復号手段、２０７は第１のインタフェースである。２０８は第２の装置であり、例えばＤＶＤである。２０９は第２のＩＤ情報、２１０は擬似乱数生成手段、２１１は第２の暗号化手段、２１２は第２の復号手段、２１３は第２のインタフェース、２１４はディジタル情報である。第２の装置２０８は、ディジタル情報２１４を暗号化して送信する。２１５は第２の装置２０８により暗号化して送信されたディジタル情報２１４を受信して復号する第３の装置であり、例えばユーザが使用するパソコンである。２１６は第３のＩＤ情報、２１７は第３の復号手段、２１８は第３のインタフェース、２１９は第１～第３の装置にそれぞれ格納されている初期値である。

【００２１】次に動作を説明する。まず、鍵情報２０２を、第１の装置２０１、第２の装置２０８及び第３の装置２１５の３つの装置で共有する手順を説明する。第１の装置２０１にはあらかじめ、固有の鍵情報２０２、第１のＩＤ情報２０３及び初期値２１９が書き込まれている。第２の装置２０８にはあらかじめ、第２のＩＤ情報２０９及び初期値２１９が書き込まれている。第３の装置２１５にはあらかじめ、第３のＩＤ情報２１６及び初期値２１９が書き込まれている。初期値２１９は、第１の装置２０１、第２の装置２０８及び第３の装置２１５において共通の値である。まず、第１の装置２０１の暗号化鍵生成手段２０４において暗号化鍵を生成し、その暗号化鍵は、第１の暗号化手段２０５により初期値２１９を暗号化鍵として暗号化され、第１のインタフェース２０７を介して第２の装置２０８及び第３の装置２１５に送信される。第２の装置２０８及び第３の装置２１５でそれが復号され、暗号化鍵生成手段２０４において生成された暗号化鍵は、システムを構成する３つの装置に固有の鍵であり、３つの装置で共有される。次に、この共有された暗号化鍵を用いて、第１の暗号化手段２０５において鍵情報２０２を暗号化し、第１のインタフェース２０７を介して第２の装置２０８及び第３の装置２１５に送信される。次に、第２の復号手段２１２及び第３の復号手段２１７において、暗号化された鍵情報２０２は復号され、鍵情報２０２は、３つの装置で共有される。

【００２２】次に、第２の装置２０８のディジタル情報２１４を、第３の装置２１５に送信する手順を説明する。まず、擬似乱数生成手段２１０において擬似乱数を生成し、生成された擬似乱数を暗号化鍵としてディジタル情報２１４を暗号化する。生成された擬似乱数は、鍵情報２０２を暗号化鍵として第２の暗号化手段２１１により暗号化する。暗号化された擬似乱数と、暗号化されたディジタル情報２１４を、第２のインタフェース２１３を介して第３の装置２１５に送信する。第３の装置２１５では、共有されている鍵情報２０２を用いて、まず暗号化された擬似乱数を復号する。次に、復号された擬似乱数を用いて、暗号化されたディジタル情報２１４を復号し、元のディジタル情報２１４を得る。本実施の形態の著作権保護システムは、ディジタル情報を送信するとき、暗号化されているので、ディジタル情報の不正な複製を防ぐことができ、著作者の権利を保護することができる。

【００２３】実施の形態４．前記実施の形態３では、第２の装置２０８及び第３の装置２１５において、共有の鍵情報２０２を保持していたが、ディジタル情報２１４

を送信するときのみ保持するようにし、送信が終了したら装置内から消去し、次の送信を開始するときに、再び共有するようにすることもできる。

【００２４】実施の形態５．前記実施の形態３では、鍵情報２０２を第２の装置２０８及び第３の装置２１５に送信するとき、初期値２１９を暗号化鍵としていたが、まず、最初の第１の装置２０１に対し、第２の装置２０８の保持する第２のＩＤ情報２０９および第３の装置２１５の保持する第３のＩＤ情報２１６を送信し、第１の装置２０１において、第１のＩＤ情報２０３と第２の装置２０８及び第３の装置２１５から送られてきた第２のＩＤ情報２０９及び第３のＩＤ情報２１６をもとに第１の装置２０１のみが保有している鍵情報２０２を秘密のパラメーターとして新たな暗号化鍵を暗号化鍵生成手段２０４において生成し、これを初期値２１９の代わりに用いることもできる。

【００２５】実施の形態６．前記実施の形態３では、鍵情報２０２を暗号化するために暗号化鍵生成手段２０５で生成した暗号化鍵は、第１の装置２０１、第２の装置２０８及び第３の装置２１５で保持されていたが、これら３つの装置のいずれかが、別の装置に入れ替わった場合は、次のようにすればよい。まず、第１のＩＤ情報２０３、第２のＩＤ情報２０９及び第３のＩＤ情報２１６を用いて、暗号化鍵生成手段２０４で新たな暗号化鍵を生成する。次に、生成された暗号化鍵を、第１の暗号化手段２０５で初期値２１９を暗号化鍵として暗号化し、第２の装置２０８及び第３の装置２１５に送信する。第２の装置２０８及び第３の装置２１５では初期値２１９を用いて復号し、暗号化鍵生成手段２０４で生成された新たな暗号化鍵は共有される。

【００２６】実施の形態７．前記実施の形態１～６の著作権保護方法及び著作権保護システムは、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｉｄｅｏ Ｄｉｓｃ）、ＣＤ－ＲＯＭなど、ディジタル情報記録媒体全般の再生装置に用いることもできる。また、第１の装置２０１は、ＩＣカードおよびＰＣカードなどの携帯型情報記録媒体としたが、鍵情報２０２を秘密に保持できる記録媒体であれば良い。

【００２７】

【発明の効果】以上のように、本発明による著作権保護方法及び著作権保護システムは、ディジタル情報の不正な複製を防ぐことができ、著作者の権利を保護することができる効果がある。

【図面の簡単な説明】

【図１】　本発明の著作権保護方法を説明する図である。

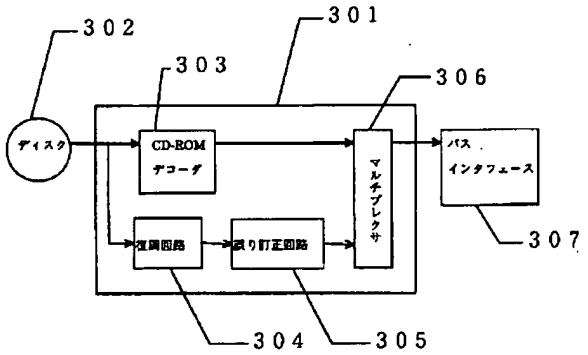
【図２】　本発明の著作権保護システムの構成図である。

【図３】　従来の光ディスクシステムの構成図である。

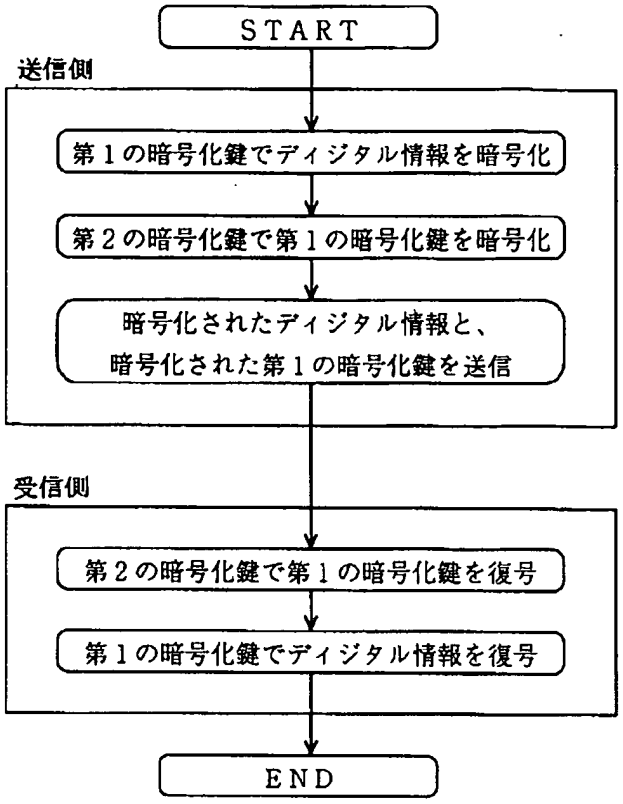
【符号の説明】

２０１　第１の装置、２０２　鍵情報、２０３　第１のＩＤ情報、２０４　暗号化鍵生成手段、２０５　第１の暗号化手段、２０６　第１の復号手段、２０７第１のインタフェース、２０８　第２の装置、２０９　第２のＩＤ情報、２１０　擬似乱数生成手段、２１１　第２の暗号化手段、２１２　第２の復号手段、２１３　第２のインタフェース、２１４　ディジタル情報、２１５　第３の装置、２１６　第３のＩＤ情報、２１７　第３の復号手段、２１８　第３のインタフェース、２１９　初期値。

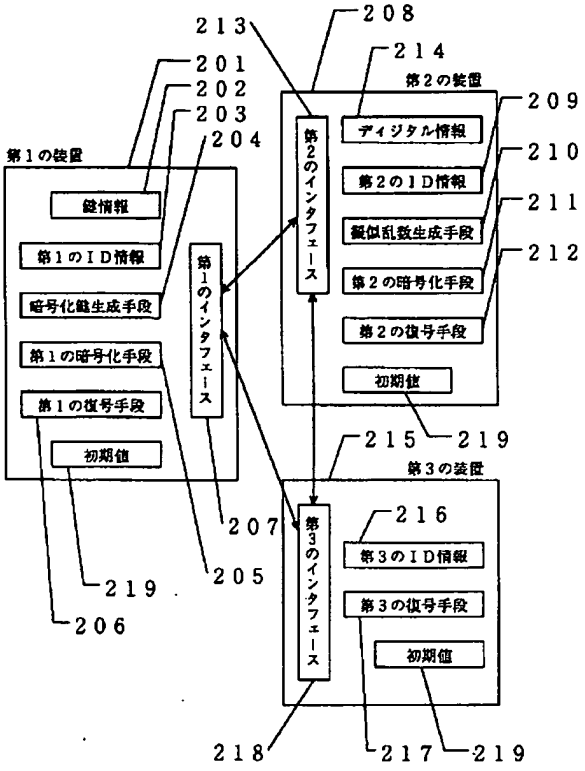
【図３】



【図1】


START
送信側
第1の暗号化鍵でディジタル情報を暗号化
第2の暗号化鍵で第1の暗号化鍵を暗号化
暗号化されたディジタル情報と、
暗号化された第1の暗号化鍵を送信
受信側
第2の暗号化鍵で第1の暗号化鍵を復号
第1の暗号化鍵でディジタル情報を復号
END

【図2】


213
208
214
201
202
203
204
第2の装置
209
第1の装置
第2のインタフェース
ディジタル情報
210
鍵情報
第1のID情報
第2のID情報
211
擬似乱数生成手段
第1のインタフェース
212
暗号化鍵生成手段
第2の暗号化手段
第1の暗号化手段
第2の復号手段
第1の復号手段
初期値
初期値
215
219
第3の装置
207
216
第3のID情報
219
205
第3のインタフェース
第3の復号手段
206
初期値
218
217
219